



BitLocker 活用マニュアル Pentio USB Token 3300A 付属パッケージ

Windows 8.1 Pro / Windows 7 Ultimate
セットアップマニュアル

2014/3/5

ペンティオ、Pentio およびそれらを含むロゴは日本および他の国におけるペンティオ株式会社の商標または登録商標です。

ジェムアルト、Gemalto およびそれらを含むロゴは日本および他の国におけるジェムアルト株式会社の商標または登録商標です。

Microsoft および Windows、Windows Vista、Windows Server は米国 Microsoft Corporation の米国、日本およびその他の国における登録商標です。

Mac OS および OS X は米国および他の国々で登録された Apple Inc.の商標です。

その他本文中に記載されている製品名および社名は、それぞれ各社の商標または登録商標です。

Microsoft Corporation のガイドラインに従って画面写真を掲載しています。

本書の著作権はペンティオ株式会社に帰属します。著作権法の認める範囲を除き、本書を無断で複製、複写、改変、デジタルデータに変換すること、および営利非営利を問わず再配布、譲渡することを禁じます。

目次

目次	4
1 はじめに	6
1.1. はじめに	6
1.2. 必要システム	6
1.2.1. スマートカード	6
1.2.2. 対応 OS	6
1.3. 必ずご確認ください	7
1.4. 全体の流れ	8
1.5. 用語について	9
2 「鍵」と「錠」を準備する	11
2.1. 「鍵」と「錠」を作ってスマートカードに書き込む	11
2.2. 書き込まれた「錠」の確認方法	13
3 暗号化ドライブにする	14
3.1. 自己署名証明書を受け入れる設定にする	14
3.2. BitLocker で暗号化する	15
3.3. 自己署名証明書を受け入れる設定を戻す	19
4 施錠する	20
5 解錠する	21
5.1. 外付けドライブを取り付ける	21
5.2. 暗号化したコンピューター以外で解錠する場合	23
5.2.1. Windows 8.1 または Windows 7 の場合	23
5.2.2. Windows Vista または Windows XP の場合	23
6 BitLocker による暗号化ドライブを元に戻す	25
6.1.1. Windows 8.1 の場合	25

1 はじめに

1.1. はじめに

このたびは Pentio USB Token 3300A / Pentio IC Card 3300C をご購入いただきましてありがとうございます。スマートカードまたはトークン（以下「スマートカード等」と表記します）を用いて外付けドライブやフラッシュメモリを暗号化する方法を解説しています。

1.2. 必要システム

1.2.1. スマートカード

ドライブの暗号化にスマートカード等を利用する場合は、「トークン」または「スマートカード読み取り装置とスマートカード」が必要です。

- トークン Pentio USB Token 3300A
- スマートカード読み取り装置 Gemalto USB Key Card Reader
- スマートカード Pentio IC Card 3300C (Gemalto)

1.2.2. 対応 OS

ドライブを BitLocker で設定するには、以下のシステムが必要です。

- Windows 8.1 Pro エディション または Enterprise エディション
- Windows 8 Pro エディション または Enterprise エディション
- Windows 7 Ultimate エディション または Enterprise エディション

BitLocker が設定されたドライブに対する操作は、以下の OS で行えます。

書き込み

- Windows 8.1 / 8
- Windows 7

読み込み

- Windows 8.1 / 8
- Windows 7
- Windows Vista
- Windows XP

Windows XP と Windows Vista では書き込みができません。暗号化されたドライブは読み取り専用としてご利用いただけます。

OS と BitLocker の対応

	Windows 8.1 / 7 上位エディション	Windows 8.1 / 7 下位エディション	Windows Vista Windows XP
BitLocker で暗号化ドライブを設定する	○	×	×
書き込み	○	○	×
読み取り	○	○	△※注意
BitLocker の設定を変更・解除する	○	×	×

※注意 これらの OS ではスマートカードでの解錠に対応していません。パスワードまたは回復キーの入力にて解錠できます。

上位エディション Windows 7 の Ultimate / Enterprise および Windows 8.1 / 8 の Pro / Enterprise を指します

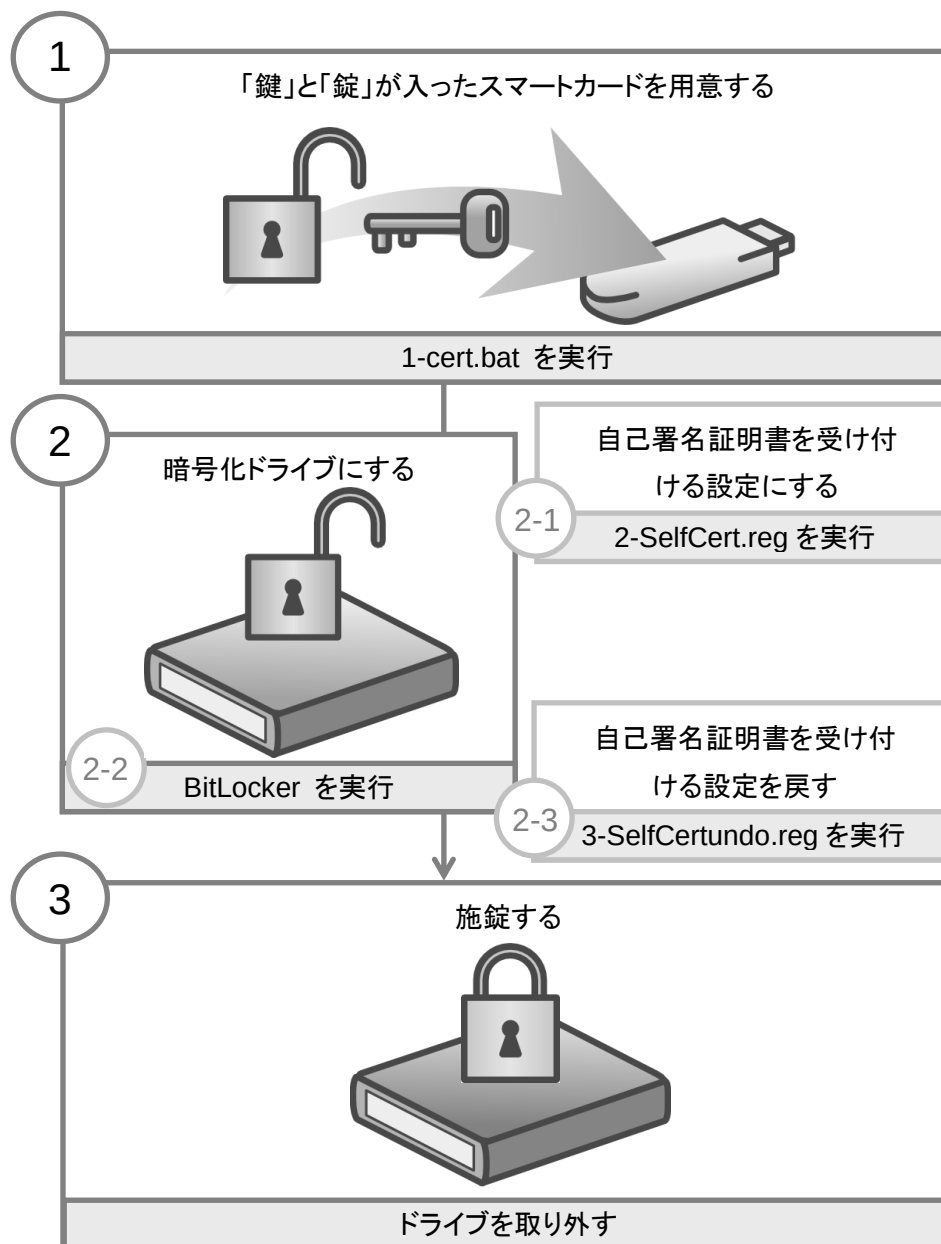
下位エディション 上記を除くエディションを指します

1.3. 必ずご確認ください

BitLocker でロックする前に、以下の点をご確認ください。

- お使いの環境がシステム要件を満たしているか確認してください。Windows 8.1 / 8（無印）や Windows 7 Home Premium、Windows 7 Professional などのエディションでは BitLocker の設定を行えません。
- スマートカード読み取り装置、スマートカード、トークンなどのセットアップは完了させておいてください。セットアップの詳細はスマートカード等の取扱説明書をご覧ください。
- 外付けドライブが正常に動作することをご確認ください。他の暗号化ソフトウェアを使用していた場合 BitLocker でのロックが正常に行われられない可能性がありますので全て解除、無効化してください。
- 以下の操作では管理者特権が必要になります。管理者特権をお持ちでない場合、システムの管理者にお問い合わせください。
- 作成する「鍵」と「錠」は、1 個の USB トークンまたは 1 個のスマートカードにのみ保存出来ます。複製はできません。

1.4. 全体の流れ



本書では下記ウェブサイトで配布しているファイルを使用し、BitLocker による暗号化を行います。インターネットに接続されていない環境の場合は **8. インターネットに接続されていない場合** (32 ページ) をご覧ください。

http://www.pentio.com/*****

同梱物: settings.txt / 1-cert.bat / 2-SelfCert.reg / 3-SelfCertUndo.reg

1.5. 用語について

本書で使用する用語は次のとおりです。Microsoft および Windows 内の表現と異なるものがありますので、適宜読み替えてください。

外付けドライブ

本書では、USB フラッシュメモリなどのリムーバブルディスクおよび外付けのハードディスクドライブのように取り外しが可能なローカルディスクを「外付けドライブ」と総称します。



暗号化する 本書での表記: 暗号化ドライブにする

BitLocker を外付けドライブに設定し、暗号化することでドライブの内容を読み取れないようにすることを「暗号化する」または「暗号化ドライブにする」と表記します。暗号化されたドライブのデータは適切な操作をしなければ読み取ることができません。



ロックする 本書での表記: 施錠する

BitLocker で暗号化ドライブにした場合、ドライブをコンピューターから取り外すと自動的に「データにアクセスできない状態」になります。これを「ロックする」または「施錠する」と表記します。



ロックを解除する 本書での表記: 解錠する

暗号化されたデータを読める状態に戻すことを「ロックを解除する」または「解錠する」と表記します。「解錠」にあたっては「鍵」が必要です。



BitLocker を無効にする 本書での表記: 暗号化ドライブを元に戻す

BitLocker によって暗号化されたドライブを元の状態に戻し、誰でもアクセスできる状態に戻すことを「BitLocker を無効にする」または「暗号化ドライブを元に戻す」と表記します。



回復キー（数字パスワード）

BitLocker でロックした場合、「スペアキー」として回復キーが発行されます。この回復キーは 48 桁のランダムな数字です。通常はこの回復キーでロックを解除することはありませんが、万一スマートカードを紛失した場合にドライブにアクセスするために必要となりますので厳重に保管してください。BitLocker では他のデバイスへの保存または印刷を推奨しています。

秘密鍵

「解錠」に使用する「鍵」のデータです。この「鍵」は秘密鍵と呼ばれ、他人に知られないように保管します。スマートカード等を用いて BitLocker でロックした場合、秘密鍵はスマートカード等の中に保管されます。スマートカード等に格納された秘密鍵は PIN を入力することで使用可能になります。



公開鍵

「施錠」に使用する「錠」のデータです。この「錠」は公開鍵と呼ばれ、一般に誰でも使うことができます。公開鍵を使って暗号化したデータは、対応する秘密鍵を使わなければ元に戻すことができません。



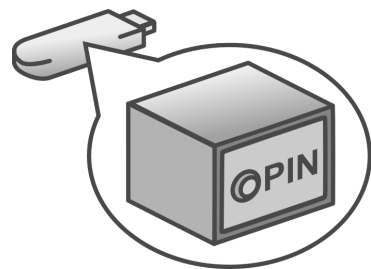
証明書

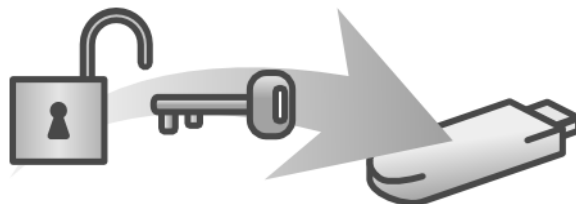
公開鍵に「誰が作ったのか」などの情報を付けたものを「証明書」と呼びます。

PIN（暗証番号、パスワード）

秘密鍵はスマートカードの「パスワードが必要な領域」に保存されます。この領域にアクセスするためにはスマートカードに設定された PIN を入力する必要があります。

PIN はスマートカードに設定されたパスワードですので、PIN を変更しても秘密鍵が書き換わることはありません。





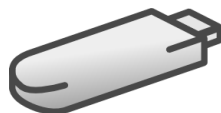
2 「鍵」と「錠」を準備する

2.1. 「鍵」と「錠」を作ってスマートカードに書き込む

スマートカード等を用いてロックする場合、ロックに使う「鍵」と「錠」(秘密鍵(鍵)と対応する公開鍵(錠)を含む証明書)を用意する必要があります。以下の手順でスマートカード等に「鍵」と「錠」のデータを書き込みます。

なお、これまでに他のドライブをロックするために作成した「鍵」と「錠」が入っているスマートカードをお持ちの場合、その「鍵」と「錠」を使用することもできます。その場合、本節の「鍵」と「錠」を作ってスマートカードに書き込む手順は必要ありません。

- 【1】 スマートカード等をコンピューターに接続します。スマートカード等の接続方法およびセットアップ方法はスマートカード等の取扱説明書をご覧ください。

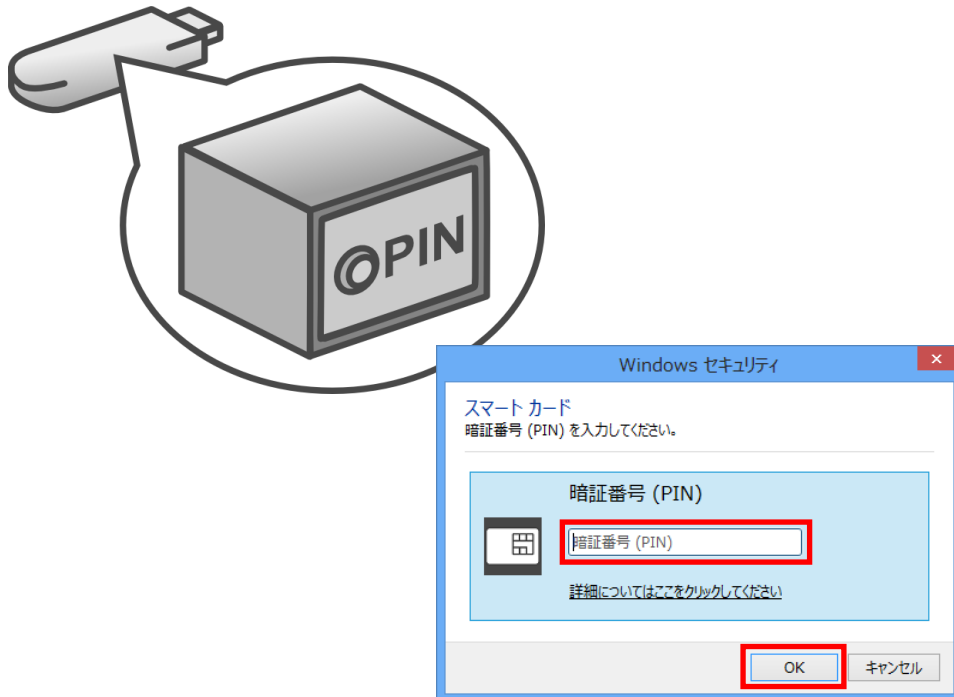


- 【2】 http://www.pentio.com/***** からダウンロードした「1-cert.bat」をダブルクリックします。コマンドプロンプトの画面が現れます。

インターネットに接続されていない場合は **8. インターネットに接続されていない場合** (32 ページ)をご覧ください。

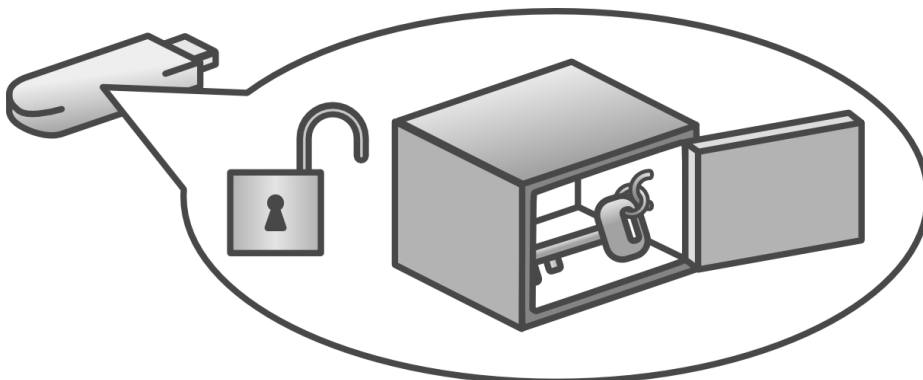


- 【3】 PIN の入力求められます。スマートカード等に設定されている PIN を入力します。



- 【4】 「鍵」と「錠」の生成と書き込みが行われます。生成と書き込みには 1 分程度かかります。その間画面に変化はありませんが、正常です（この間、カードへのアクセスが行われます）。

- 【5】 「鍵」と「錠」の生成と書き込みが完了すると、コマンドプロンプトの黒い画面が閉じます。これで必要な「鍵」と「錠」のデータがスマートカードに書き込まれました。「錠」を使用する際に PIN は不要ですが、「鍵」へのアクセスは PIN が必要です。また、「鍵」のデータをスマートカードから取り出すことはできません。



- 【6】 「1-cert.bat」と同じディレクトリに「req.req」が生成しますが、削除して構いません。

2.2. 書き込まれた「錠」の確認方法

本手順は通常であれば必要ありません。

- 【 1 】** Internet Explorer を起動します。
- 【 2 】** 「ツール」の「インターネット オプション」をクリックします。
- 【 3 】** 「コンテンツ」タブの「証明書」をクリックします。
- 【 4 】** 「目的:<すべて>」を選び、「個人」タブを選択します。発行先が BitLocker となっている証明書があることを確認します。



3 暗号化ドライブにする

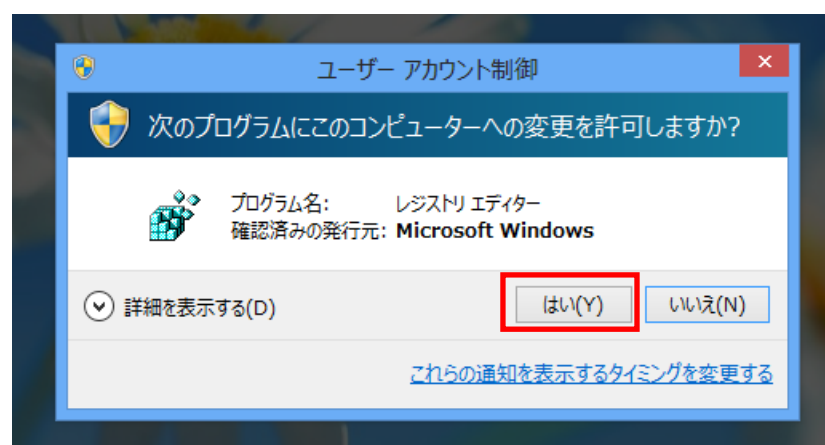
3.1. 自己署名証明書を受け入れる設定にする

前章で作成した「錠」(公開鍵を含む証明書)は「自己署名証明書」と呼ばれます。自己署名証明書は信頼できる第三者からのお墨付き(署名)がなく、「誰が作ったのか」が信用できません。そのため通常 Windows では自己署名証明書利用を認めない設定になっています。今回は自分で作成した信頼できるものを使用しますので、次の手順で一時的に「自己署名証明書を受け入れる」設定にします。

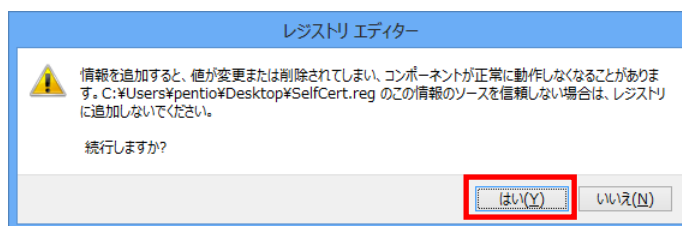
- 【1】 http://www.pentio.com/***** からダウンロードした「2-SelfCert.reg」をダブルクリックします。

(インターネットに接続されていない場合は **8. インターネットに接続されていない場合** (32 ページ)をご覧ください)

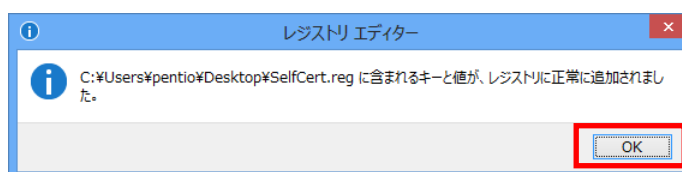
- 【2】 警告が表示されますので、「はい」をクリックします。



- 【 3 】 警告が表示されますので、「はい」をクリックします。



- 【 4 】 正常に書き込みが完了した旨が表示されます。「OK」をクリックします。

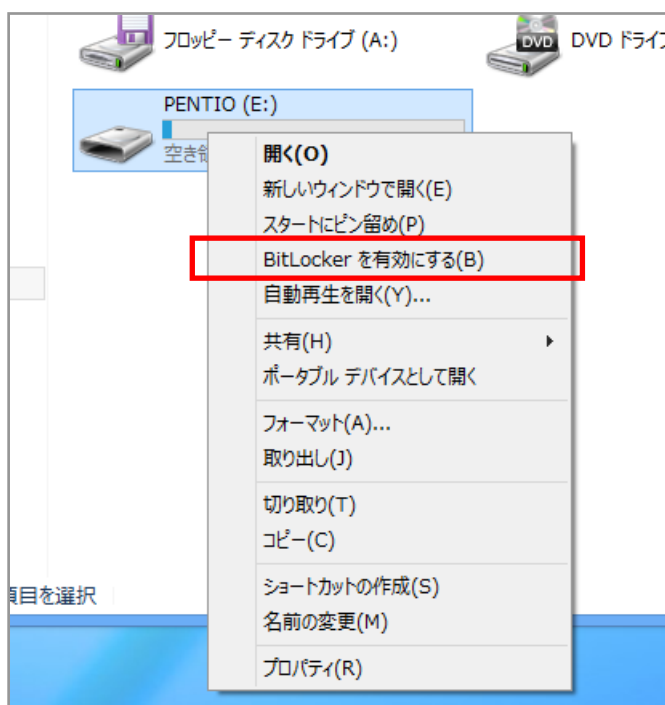


以上で自己署名証明書、すなわち自作の「錠」を使う準備ができました。

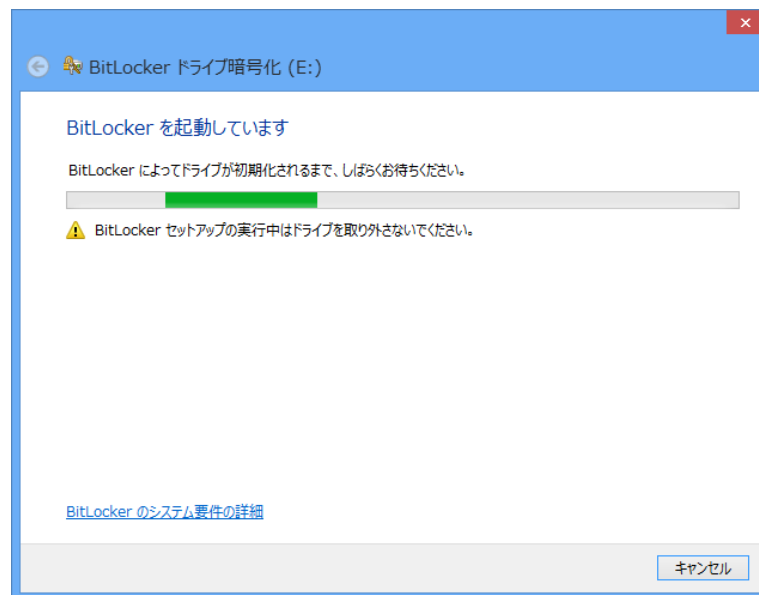
3.2. BitLocker で暗号化する

作成した「錠」(公開鍵を含む証明書)を使って外付けドライブを暗号化ドライブにします。

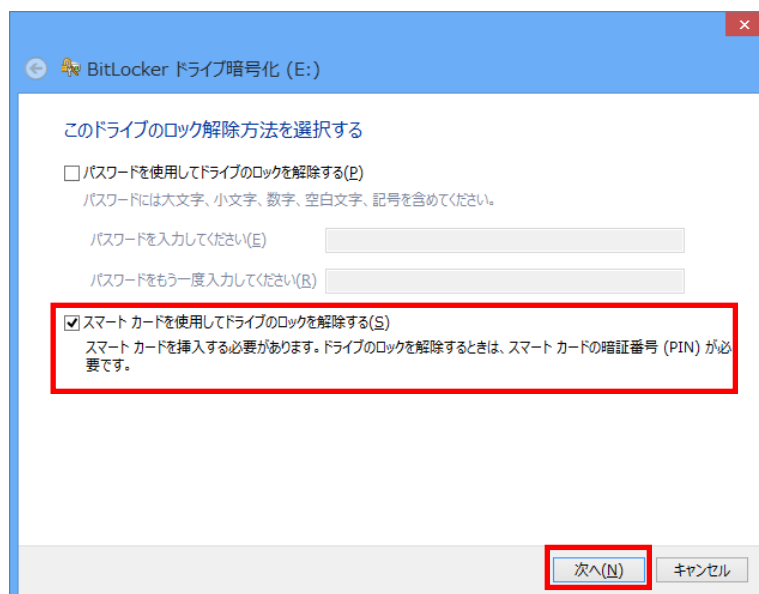
- 【 1 】 ロックする外付けドライブを接続し、「コンピューター」を開きます。
- 【 2 】 ロックしたいドライブを右クリックし、「BitLocker を有効にする」をクリックします。



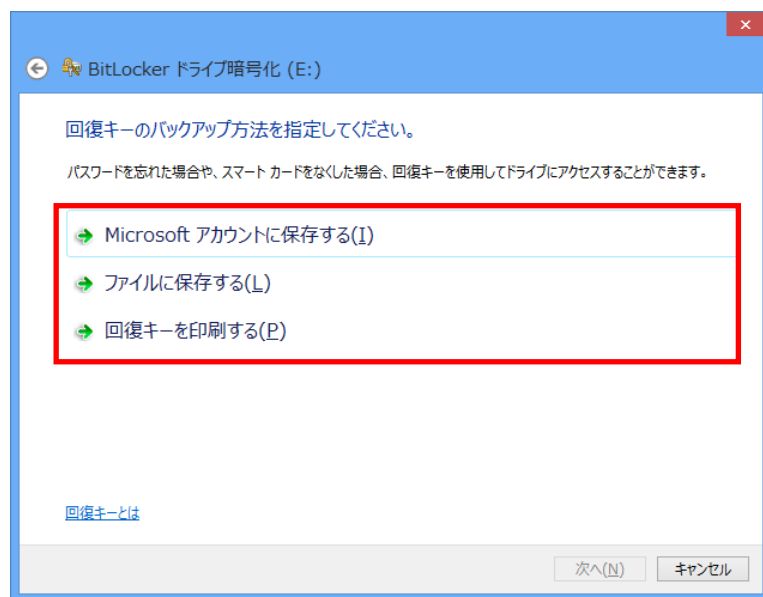
- 【 3 】 BitLocker が起動します。起動には数十秒程度かかることがあります。



- 【 4 】 ロックの方法を指定します。パスワードによるロックとスマートカードによるロックの一方または両方を選択できます。ここでは「スマートカードを使用してドライブのロックを解除する」を選択し、「次へ」をクリックします。



- 【5】 スマートカードに BitLocker 用の証明書が複数含まれる場合、「証明書の選択」画面が表示されます。選択して「OK」をクリックします。
- 【6】 回復キーの保存方法を指定します。回復キーはロックを解除できる長いパスワードです。万が一スマートカードを紛失した場合、この回復キーを用いてデータにアクセスできます。いわばスペアキーですので、確実に保存・印刷してください。回復キーとスマートカードの両方を失うと、データにアクセスできなくなります。



Windows 7 では保存先として Microsoft アカウントは表示されません

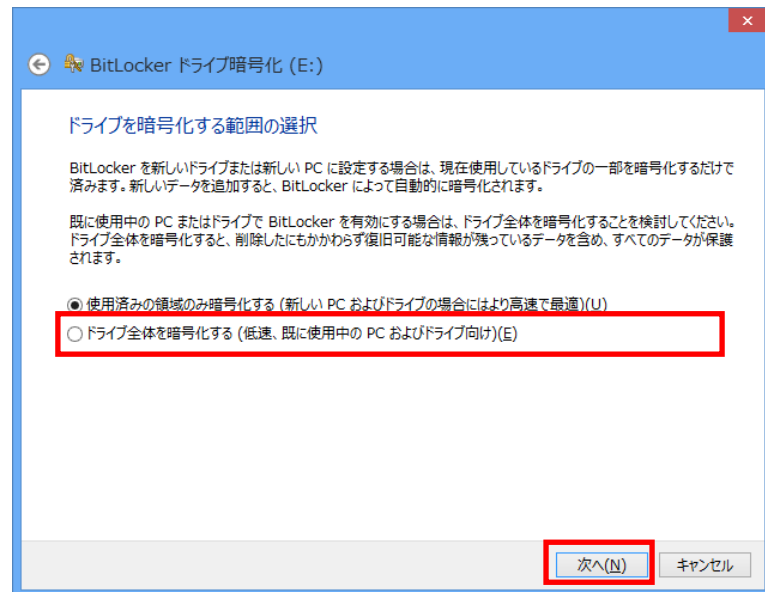
- 【7】 回復キーの保存と印刷は「次へ」をクリックするまで、両方を何度でも行えます。

回復キーを印刷して保管することを強く推奨します。

- 【8】 回復キーを保管したら、「次へ」をクリックします。

- 【 9 】** Windows 8.1 / 8 では「使用中の領域の暗号化」と「ドライブ全体の暗号化」を選択できます。「使用中の領域の暗号化」は高速ですが、削除されたデータを読み取られる危険性があります。「ドライブ全体の暗号化」では時間を要しますが、セキュリティは強固です。わからなければ「ドライブ全体を暗号化する」を選択してください。

Windows 7 ではこの画面は表示されません。「ドライブ全体を暗号化する」設定で暗号化が実行されます。



- 【 10 】** 「次へ」(Windows 7 では「暗号化の開始」)をクリックすると暗号化が開始されます。



- 【 11 】** 処理は一時停止できます。また、処理の間も通常通りデータにアクセスできます。

- 【 12 】** ロックが完了したら以下の画面が表示されます。「閉じる」をクリックします。

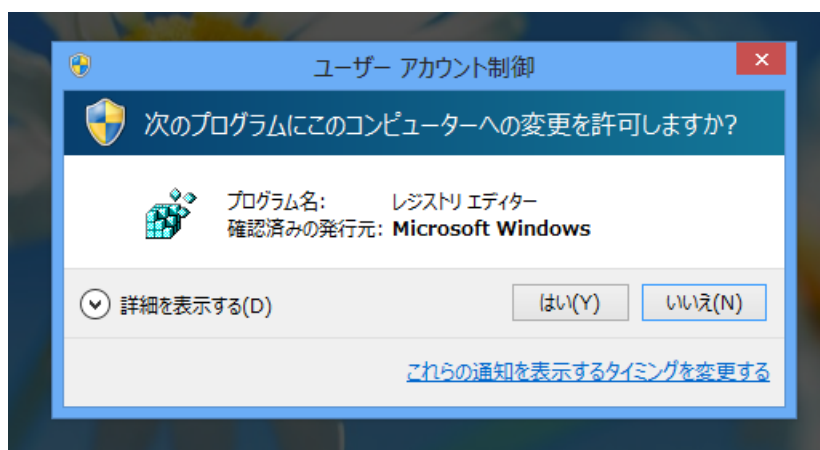


- 【13】 暗号化処理が完了したらスマートカードを取り外して構いません。

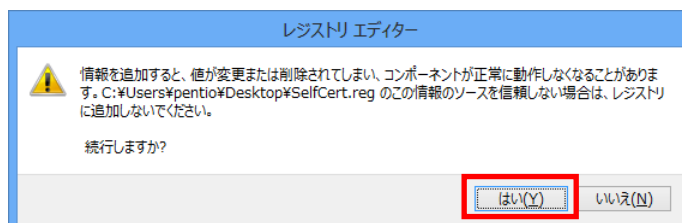
3.3. 自己署名証明書を受け入れる設定を戻す

暗号化の際に自己署名証明書を受け入れる設定にしたため、これを戻します。

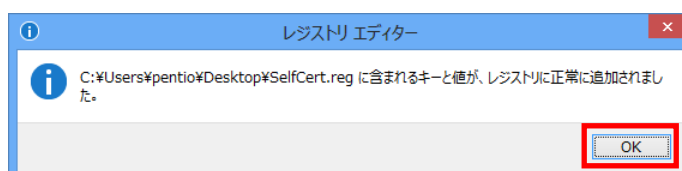
- 【1】 ダウンロードした「3-SelfCertUndo.reg」をダブルクリックします。先の手順と同様に警告が表示されますので、「はい」をクリックします。



- 【2】 警告が表示されますので、「はい」をクリックします。



- 【3】 正常に書き込みが完了した旨が表示されます。「OK」をクリックします。



以上でドライブの暗号化は完了です。

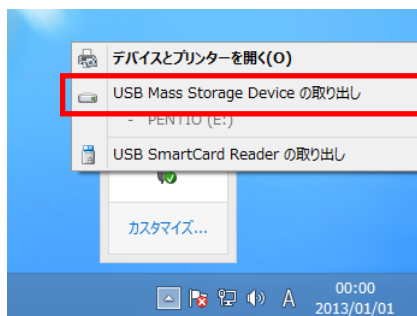


4 施錠する

BitLocker で暗号化したドライブは、次のいずれかの手順で「施錠」できます。

- コンピューターからドライブを取り外す
- Windows をシャットダウンする

ドライブを取り外す際は、必ず「ハードウェアの安全な取り外し」を行ってください。暗号化されたドライブをいきなり取り外すとデータが破損しドライブにアクセスできなくなることがあります（暗号化ドライブのデータが破損すると、復元はできません）。



施錠されたドライブにアクセスするためには、次章の「解錠」操作を行う必要があります。



5 解錠する

5.1. 外付けドライブを取り付ける

- 【1】** BitLocker でロックしたドライブをコンピューターに接続すると、ロックの解除を求める画面が表示されます。

ドライブ E: のロックを解除する
このドライブは BitLocker で保護されています。

- 【2】** ロックの解除に必要なスマートカード等を接続します。スマートカード内のデータの読み込みには数秒かかりますので、接続後 10 秒ほど待ってから[3]に進んでください。
- 【3】** 「スマートカードを使用する」をクリックします。もし「スマートカードが挿入されていない」旨の警告が表示された場合は、一度スマートカードを抜き差し直し、10 秒ほど待ってから再度お試しください。

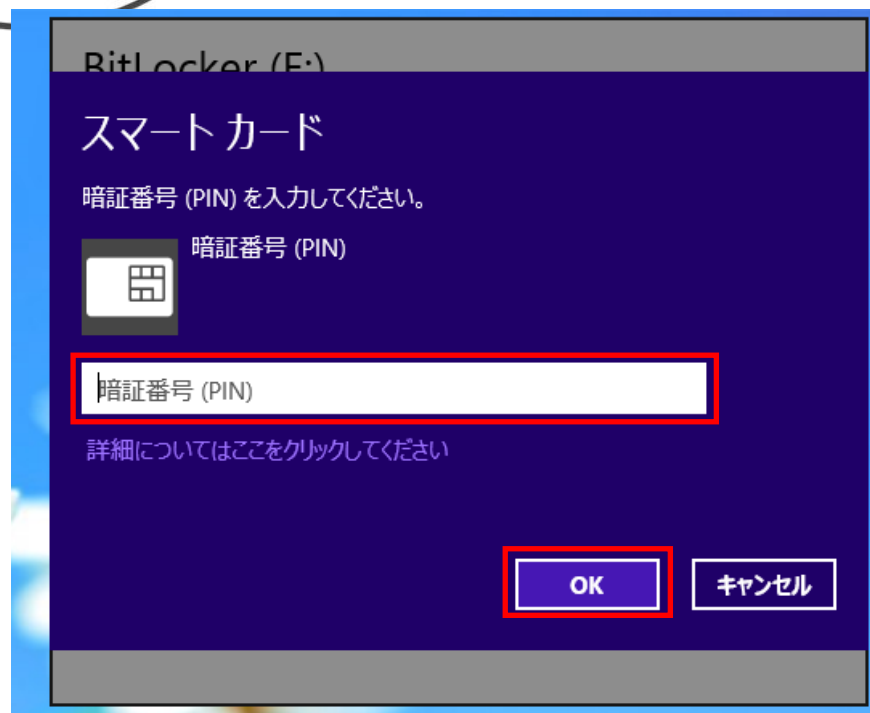
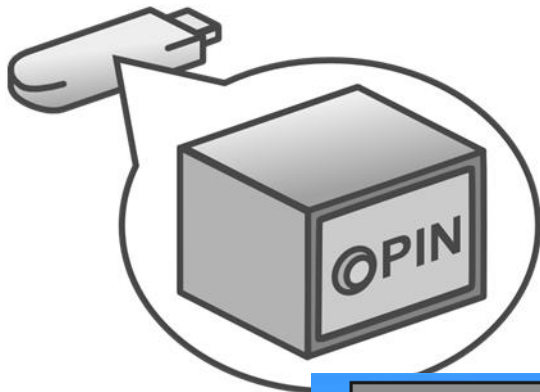
BitLocker (E:)

スマートカードを使用する

回復キーを入力する

☐ この PC で自動的にロックを解除する

- 【4】 PIN の入力を求められるので、カードの PIN を入力します。



- 【5】 ロックが解除され、データにアクセスできます。このドライブにデータを書き込むと、自動的に暗号化されます。

5.2. 暗号化したコンピューター以外で解錠する場合

BitLocker で「施錠」したドライブは、他のコンピューターでも「解錠」できます。

5.2.1. Windows 8.1 または Windows 7 の場合

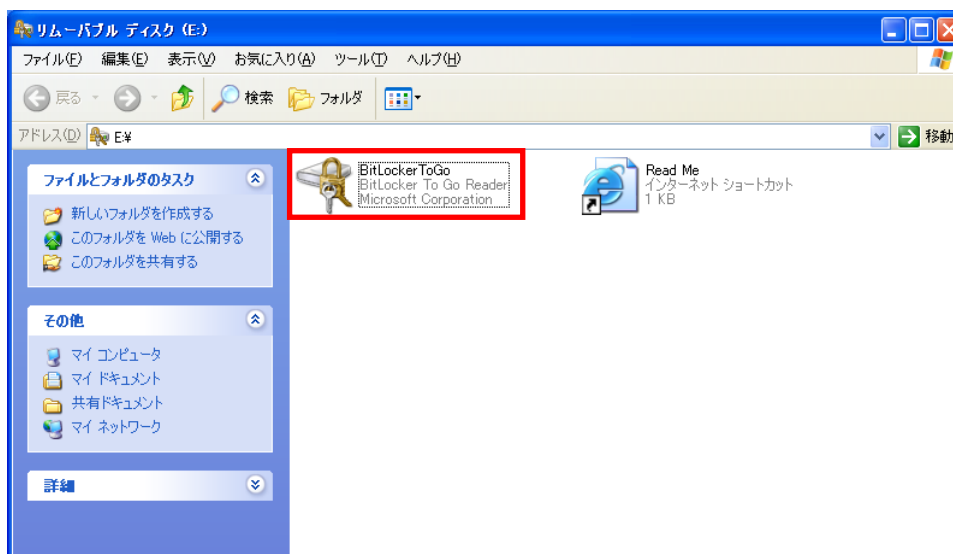
ドライブを接続すると BitLocker が起動し、ロックの解除を求める画面が表示されます。

- 【1】 解除に必要なスマートカード等を接続し、「解除する」をクリックします。
- 【2】 PIN の入力を求められるので、カードの PIN を入力します。
- 【3】 ロックが解除され、データにアクセスできます。このドライブにデータを書き込むと、自動的に暗号化されます。

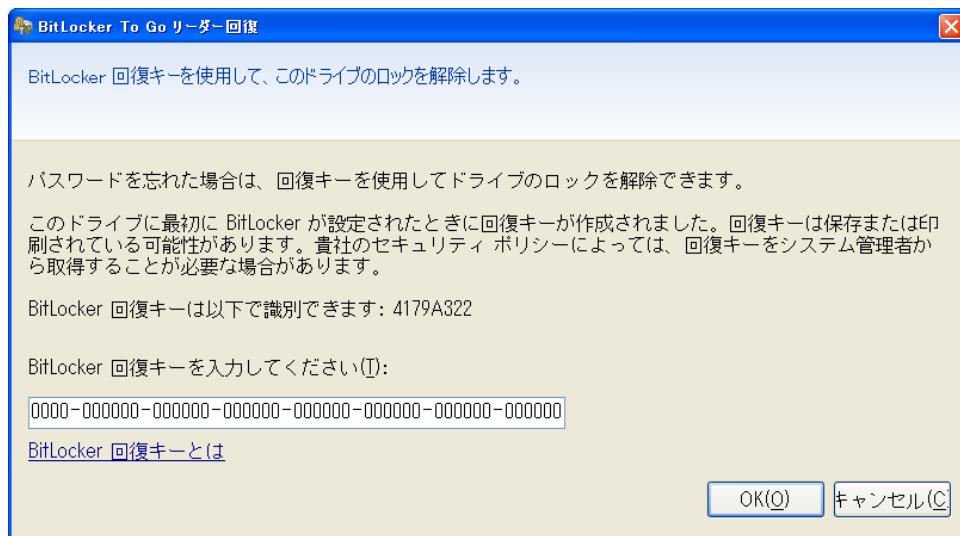
5.2.2. Windows Vista または Windows XP の場合

Windows Vista または Windows XP の場合、「解錠」にスマートカードを使用することができません。ロックの解除にはパスワードもしくは回復キーが必要です（ロックの解除方法としてスマートカードのみを指定している場合は、48 桁の回復キーを入力する必要があります）。

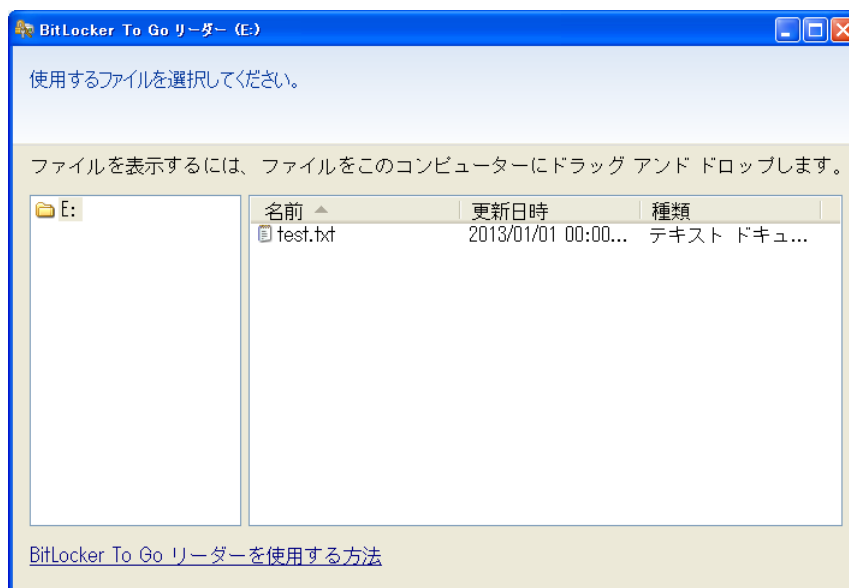
- 【1】 ドライブを接続すると、BitLocker To Go が起動します。（自動的に起動しない場合は「マイコンピューター」から目的のドライブを開き、「BitLockerToGo」を実行してください）



- 【2】 パスワードまたは回復キーを入力し、「OK」をクリックします。



- 【3】 BitLocker To Go リーダーが起動します。読み込みたいファイルを選択し、ドラッグアンドドロップすることで取り出すことができます。



- 【4】 Windows VistaまたはWindows XP では暗号化されたドライブにデータを書き込むことはできません。



6 BitLocker による暗号化ドライブを元に戻す

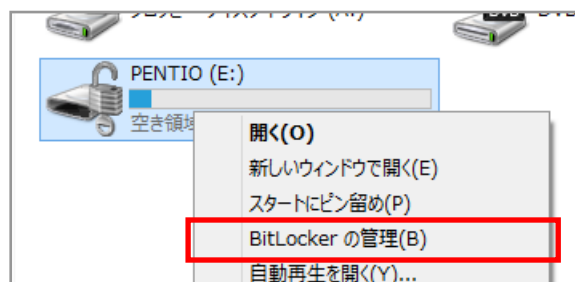
本章では BitLocker による暗号化ドライブを元に戻す方法を記載します。この手順を行うと BitLocker による保護は無効になり、誰でもドライブにアクセスできるようになります。

以下の操作は Windows 8.1 Pro エディション もしくは Enterprise エディション、または Windows 7 Ultimate エディション もしくは Enterprise エディションでのみ行えます。

なお、解錠の方法を変更する場合は [7. 「解錠」の方法を変更する](#) (29 ページ) をご覧ください。

6.1.1. Windows 8.1 の場合

- 【 1 】 「コンピューター」を開きます。
- 【 2 】 BitLocker でロックされたドライブを右クリックし、「BitLocker の管理」をクリックします。「BitLocker ドライブ暗号化」ウィンドウが開きます。（「BitLocker ドライブ暗号化」ウィンドウは「検索チャーム」に「BitLocker」と入力することでも起動できます）



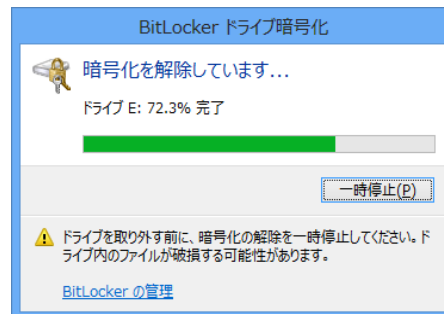
- 【3】 目的のドライブの欄に表示されている「BitLocker を無効にする」をクリックします。



- 【4】 ダイアログボックスが表示されます。「BitLocker を無効にする」または「ドライブの暗号化解除」をクリックします。



- 【5】 暗号化の解除が行われます。



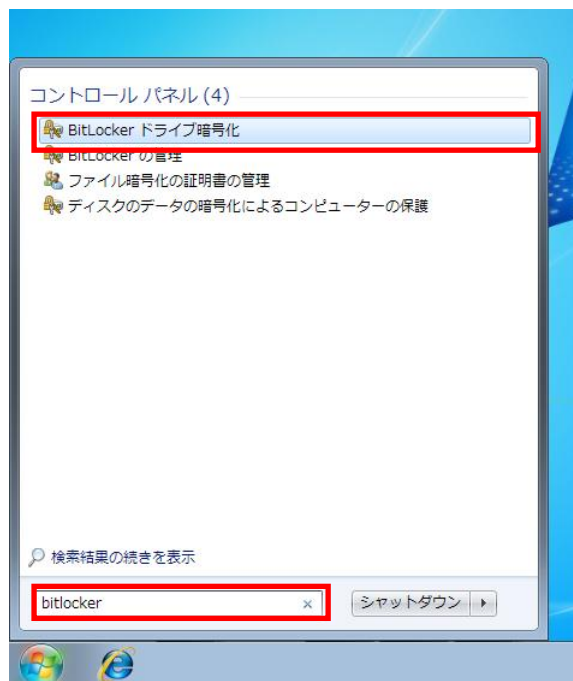
- 【6】 「閉じる」をクリックします。



以上でドライブの暗号化は無効になりました。

6.1.2. Windows 7 の場合

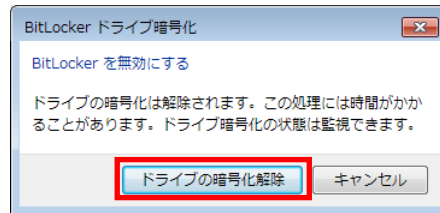
- 【1】 スタートメニューの検索欄に「BitLocker」と入力します。検索結果の「BitLocker ドライブ暗号化」をクリックします。「BitLocker ドライブ暗号化」が起動します。



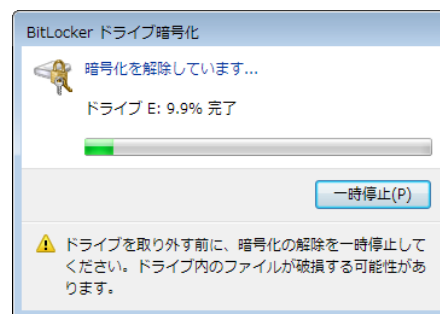
- 【2】 コンピューターに接続されているドライブの一覧が表示されます。目的のドライブの欄に表示されている「BitLocker を無効にする」をクリックします。



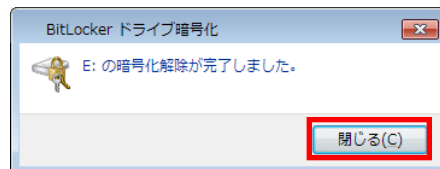
- 【3】 ダイアログボックスが表示されます。「ドライブの暗号化解除」をクリックします。



- 【4】 暗号化の解除が行われます。



- 【5】 「閉じる」をクリックします。



以上でドライブの暗号化は無効になりました。

7 「解錠」の方法を変更する

BitLocker による暗号化後も、「解錠」の方法を変更できます。例えば解錠の方法としてパスワードを設定したりスマートカードを別のものに変更したりできます。

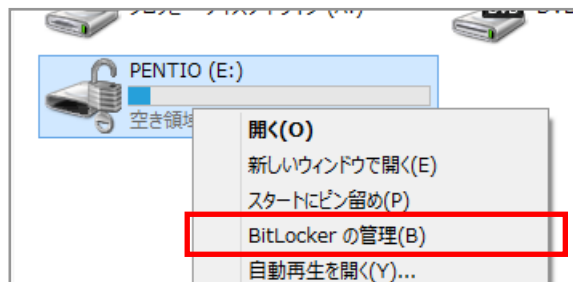
なお、複数のパスワードや複数のスマートカードを指定することはできません。また、パスワードとスマートカードの両方を削除することもできません。BitLocker による暗号化を無効にする場合は前章 [6. BitLocker による暗号化ドライブを元に戻す](#)（25 ページ）をご覧ください。

以下の操作は Windows 8.1 Pro エディション もしくは Enterprise エディション、または Windows 7 Ultimate エディション もしくは Enterprise エディションでのみ行えます。

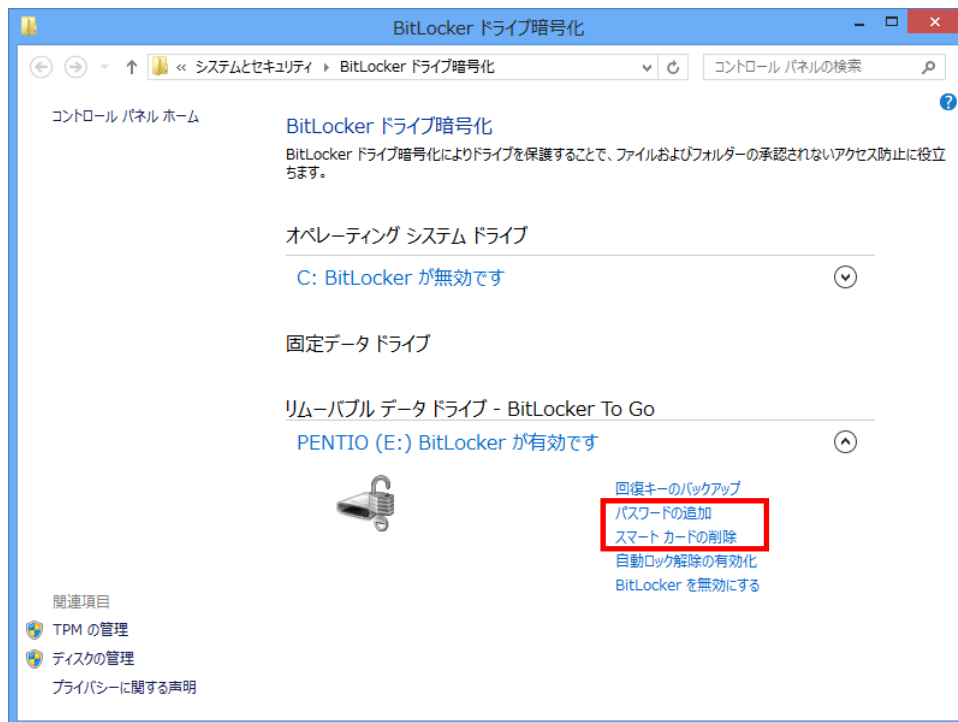
7.1.1. Windows 8.1 の場合

- 【1】 「コンピューター」を開きます。
- 【2】 BitLocker でロックされたドライブを右クリックし、「BitLocker の管理」をクリックします。「BitLocker ドライブ暗号化」ウィンドウが開きます。

「BitLocker ドライブ暗号化」ウィンドウは「検索チャーム」に「BitLocker」と入力することでも起動できます

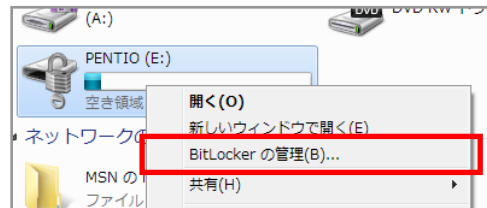


- 【3】 目的のドライブの欄に表示されている「パスワードの追加(削除)」「スマートカードの追加(削除)」をクリックすることでパスワードおよびスマートカードを追加または削除できます。

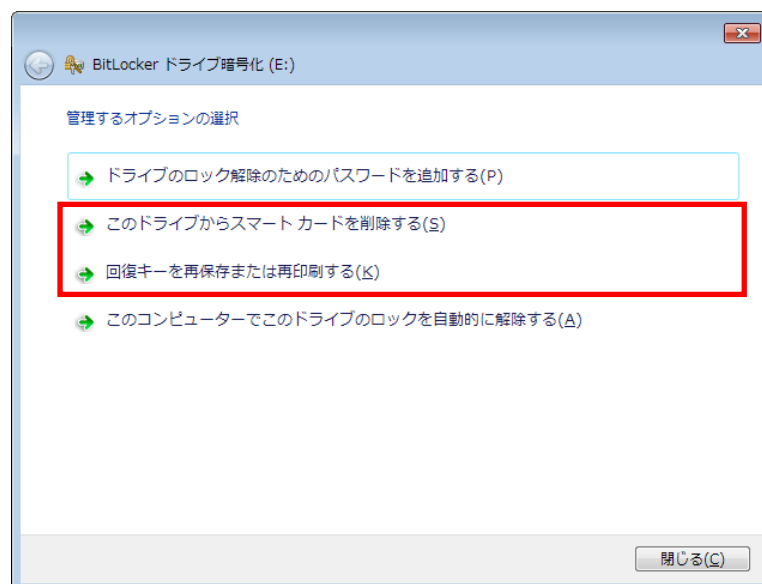


7.1.2. Windows 7 の場合

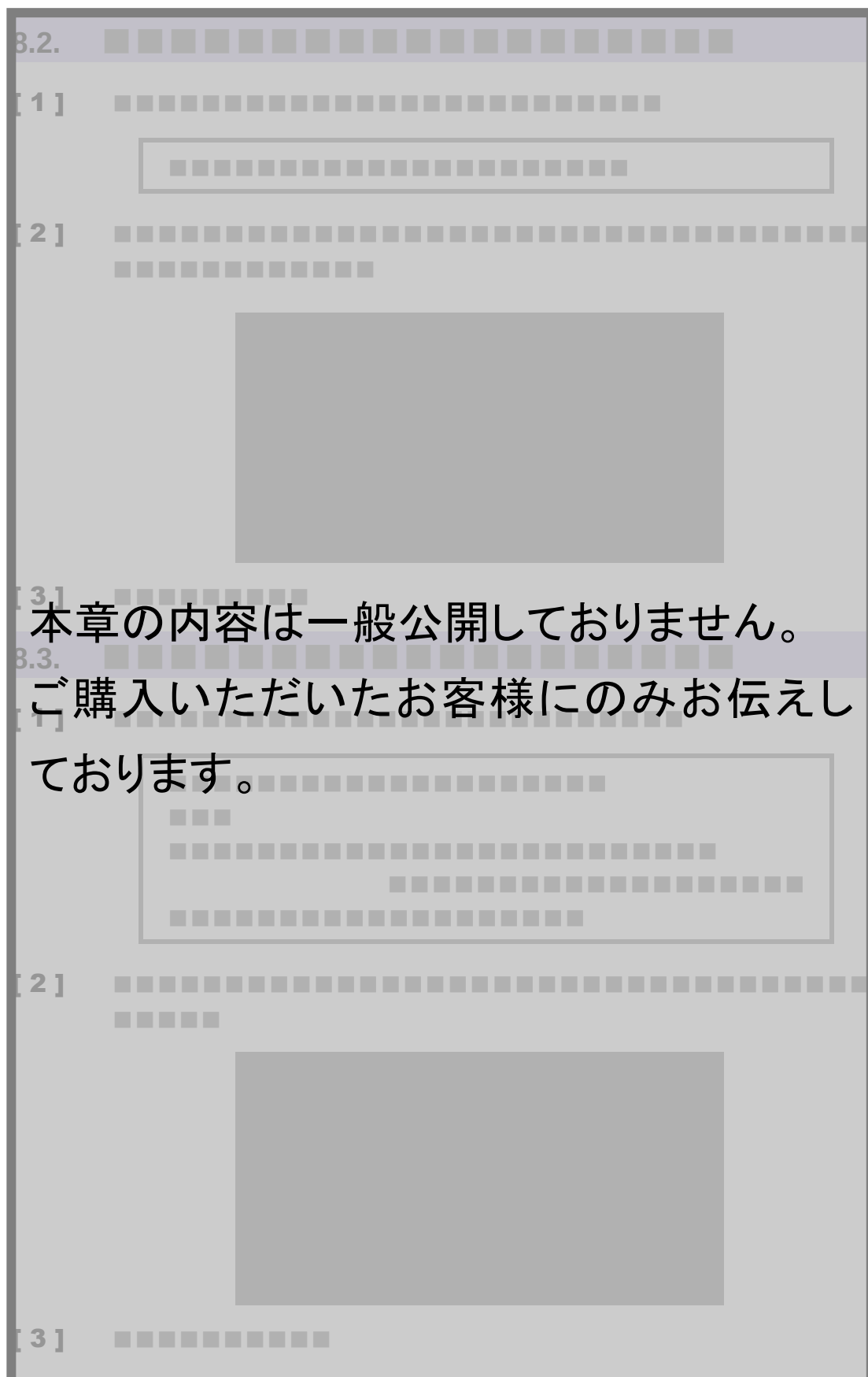
- 【 1 】 「コンピューター」を開きます。
- 【 2 】 BitLocker でロックされたドライブを右クリックし、「BitLocker の管理」をクリックします。「BitLocker ドライブ暗号化」ウィンドウが開きます。



- 【 3 】 「パスワードの追加(削除)」「スマートカードの追加(削除)」をクリックすることでパスワードおよびスマートカードを追加または削除できます。



本章の内容は一般公開しておりません。
ご購入いただいたお客様にのみお伝えしております。



3.4. [1]

[2]

本章の内容は一般公開しておりません。
ご購入いただいたお客様にのみお伝えして
おります。

9 設定がうまくいかない時は

9.1. 「鍵」と「錠」の生成に関して

メモ帳で作成した cert.bat をダブルクリックすると、「指定されたファイルが見つかりません」というエラーメッセージが表示される

→ cert.txt のファイル名は正しいですか？括弧子を表示しない設定になっている場合、cert.txt は「cert」と表示されます。

→ cert.bat の記述は正しいですか？スペルミスの可能性が考えられます。

→ 上記で解決しない場合、http://www.pentio.com/***** からファイルをダウンロードしてお使いください。

書き込みが成功したかわからない

→ 次の手順でスマートカード内の証明書(「錠」)を表示します。

インターネットエクスプローラーを開き、「ツール」→「インターネットオプション」の順にクリックします。「コンテンツ」タブの「証明書」をクリックします。「証明書」ウィンドウの「個人」タブに「BitLocker」が表示されていれば必要な「鍵」と「錠」は書き込まれています。表示されていない場合は再度「鍵」の生成を行なってください。

9.2. 自己署名証明書の許可に関して

「～¥SelfCert.reg をインポートできません。指定されたファイルはレジストリファイルではありません。(略)」というエラーメッセージが表示される。

→ 作成した SelfCert.reg が正しくありません。スペルミスの可能性が考えられます。

→ 「メモ帳」で作成しましたか？他のエディターを用いた場合、文字コードや改行コードが不適切な場合があります。

→ 上記で解決しない場合、http://www.pentio.com/***** からファイルをダウンロードしてお使いください。

「～¥SelfCert.reg をインポートできません。(中略) この操作を行うのに十分な特権がありません」というエラーメッセージが表示される。

→この操作には管理者特権が必要です。管理者アカウントでログオンして操作してください。

＜「レジストリエディタ」をお使いになる場合＞

HKEY_LOCAL_MACHINE¥SOFTWARE¥Policies¥Microsoft¥FVE に移動します。(「FVE」が存在しない場合は「Microsoft」を右クリックし、「新規」→「キー」で新しいキーを作り名前を「FVE」とします)

「新規」→「DWORD(32ビット値)」をクリックし、値の名前を「SelfSignedCertificates」とします。生成した「SelfSignedCertificates」をダブルクリックし、値に「1」を入力します。(自己署名証明書を受け付けない設定に戻す場合、値を 0 にします)

9.3. BitLocker での「施錠」に関して

「BitLocker に適した証明書がスマートカードで見つかりません」というエラーメッセージが表示される

→「鍵が書き込まれていない」か「自己署名証明書を受け付けない設定になっている」ことが考えられます。それぞれ 2. 「鍵」と「錠」を準備する(11 ページ)、3.1. 自己署名証明書を受け入れる設定にする(14 ページ)をご覧ください。

10 Q&A

Q. 「鍵」を複製できますか？

A. いいえ、できません。スマートカードに含まれる秘密鍵を取り出すことはできません。

Q. 複数のスマートカードで暗号化を解除できるように設定できますか？

A. いいえ、できません。BitLockerで暗号化の解除に使えるスマートカードは一つのみです。

Q. スマートカードを紛失してしまったのですが……

A. 48桁の回復キーを入力することで暗号化を解除できます。なお、暗号化を解除した状態では BitLocker の設定を変更することができます。

Q. スマートカードを変更したい

A. **7. 「解錠」の方法を変更する** (29 ページ)をご覧ください。「スマートカードとパスワードのいずれも設定されていない」ということはできませんので、まず一時的にパスワードとスマートカードの両方で解錠できるようにします。パスワードを設定したら、現在のスマートカードを削除します。次に「スマートカードの追加」を行うことで新たなスマートカードに変更することができます。最後にパスワードを削除してください。

Q. BitLocker で暗号化したドライブを Windows XP で使えますか？

A. 対応 OS (6 ページ) をご覧ください。Windows XP および Windows Vista では読み取り専用としてご利用いただけます。

Q. BitLocker で暗号化したドライブに対して、ウイルスのスキャンは実行出来ますか？

A. 「施錠」された状態ではどんなソフトウェアもアクセスすることができません。セキュリティソフトウェアも例外ではなく、施錠された状態のドライブをスキャンすることはできません(もちろんこの状態ではウイルスも活動できません)。スマートカードなどで「解錠」すると通常のドライブと同じようにアクセスできるようになるためウイルススキャンが可能となります

お問い合わせ



ペンティオ株式会社

PKI ソリューション事業部

Tel: 03-5919-0971

Mail: sales@pentio.com

Site: <http://www.pentio.com>